Ser. No. 09/743,653
Internal Docket No. RCA 89131
CUSTOMER NO. 24498

Remarks/Arguments

Claims 1-4 and 6-17 are pending.

Claims 1-4, 6 and 15-17 stand rejected.

Claims 7-14 stand withdrawn.

No claims have been amended.

Election/Restrictions

The Examiner correctly notes that Applicant elected, without traverse, the claims of Species A, that is, claims 1-4, 6 and 15-17, for further examination.

Rejection of claims 1-4 and 15-17 under 35 USC 103(a) as being unpatentable over Kudelski (US Pat No 5144663) in view of Saito (U.S. Pat No. 5740246)

Applicants submit that for the reasons discussed below claim 1 is not unpatentable under 35 USC 103(a) over Kudelski in view of Saito.

Claim 1 reads as follows:

> A method for managing access to a restricted transmitted event, said method comprising:
>
> receiving encrypted access information associated with said transmitted event from a particular one of a plurality of service providers, said access information being encrypted using a shared public key that is shared among the plurality of service providers, said access information comprising data corresponding to the cost of said transmitted event;
>
> decrypting said access information in a conditional access module using a private key associated with the shared public key;
>
> verifying, in said conditional access module, that the cost of said transmitted event is less than a pre-stored cash reserve;
>
> receiving said transmitted event from said service provider, said transmitted event being scrambled; and
>
> descrambling said transmitted event in said conditional access module.

The invention of claim 1 resides, in part, in the recognition by the inventors that a user of digital television services may want a mix of services from several different service providers, each of whom requires either the use of a separate set-

top box or a separate smart card (specification; page 1, lines 22-30). A user would thus be required to purchase multiple conditional access smart cards and to swap the cards as the user channel surfs (specification; page 1, lines 33-36). The invention as recited in claim 1 overcomes the problem by providing a method for managing access to a restricted transmitted event, the method comprising, inter alia:

> receiving encrypted access information associated with said transmitted event from a particular one of a plurality of service providers, said access information being encrypted using a shared public key that is shared among the plurality of service providers . . .
>
> decrypting said access information in a conditional access module using a private key associated with the shared public key

Thus, the method of claim 1 provides for using a **shared public key** that is **shared among the plurality of service providers** to encrypt access information, and using a private key associated with the shared public key to decrypt the access information. The claimed method overcomes the problem of requiring the user to purchase multiple conditional access smart cards and swap cards in order to access information received from different ones of the plurality of service providers.

Kudelski teaches a method and apparatus for implementing a pay television system, wherein code words generated by random number generator 26, and information relating to the identification to be transmitted, are used to generate a scrambled signal (col. 3, line 65 - col. 4, line 4). The code word and the information are recovered at the receiver device to descramble the signal.

The Examiner acknowledges that "Kudelski does not explicitly disclose using a public key system for encrypting the access information, where the public key is shared." (Office Action, page 3). In fact, Kudelski does not disclose, either explicitly **or implicitly**, using a public key system for encrypting access information. Furthermore, Kudelski neither discloses nor suggests the following limitation of claim 1: "receiving encrypted access information associated with said transmitted event from a particular one **of a plurality of service providers**, said access information being encrypted using a shared public key **that is shared among the plurality of service providers.**"

The Examiner further states that Kudelski "... discloses that the encrypted access information may be encrypted using any encryption system," referring to col. 4, lines 54-57 of Kudelski. However, col. 4, lines 54-57 of Kudelski read as follows:

> The code for the permutation is transmitted in enciphered form, e.g. according to the system DES but not exclusively, this system DES being practically unbreakable.

This statement is not the equivalent of "the encrypted access information may be encrypted using any encryption system."

The Examiner cites Saito as disclosing a cryptographic system for conditional access that includes a charging center when data is provided on a pay basis. The Examiner further states that Saito further includes encrypting a symmetric key with a public key at the sender and decrypting the symmetric key with the corresponding private key at the receiver, where the symmetric key is used to encrypt (or scramble) program data in the conditional access system, referencing, for example, col. 14, line 56 to col. 15, line 33. The Examiner states that Saito further discloses that the public key is common to all service providers; the Examiner refers to col. 13, lines 44-58, and characterizes this portion of Saito as disclosing that the data managing center supplies the public key for all the data. The Examiner states that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kudelski by encrypting the access information with a shared public key, in order to prevent unjustified use of data and copyright management in a pay per view or video on demand system.

Applicants respectfully disagree with the characterization of the teachings of Saito. In fact, Saito, like Kudelski, fails to teach or suggest "a plurality of service providers" and "access information being encrypted using a shared public key that is shared among the plurality of service providers." As noted above, the Examiner cites col. 13, lines 44-58 of Saito as teaching "the public key is common to all service providers." However, Saito teaches a sole service provider, as may readily be appreciated by examination of: (1) Figure 2, where broadcasting station 11 is the sole service provider; (2) Figure 3, where CATV station 21 is the sole service provider; and (3) Figure 4, where CATV station 31 is the sole service provider.

The portion relied upon by the Examiner, col. 13, lines 44-58, relates to the embodiment of Figure 4, where CATV station 31 is the sole service provider. That portion reads as follows:

> The data managing center 33 prepares and supplies to the CATV broadcasting station 31 the public-key Kbd and the private-key Kvd common in all the data to be supplied and the secret-key Ksdi which is different from one data to another. The CATV station 31 encrypts the received secret-key Ksdi by using the public-key Kbd of the data managing center 33:
>
> Cksdikbd=E(Kbd,Ksdi)
>
> and broadcasts it by multiplex teletext broadcasting using scanning lines during the retrace line blanking interval of the analog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM multiplex broadcasting, or digital data broadcasting.

Thus, there is only one service provider, CATV station 31, referenced in the cited portion of Saito. In this embodiment, Saito discloses that the data managing center 33 supplies the public key to the one and only service provider, namely, CATV station 31. While Saito states that the public key is common to all **data**, there is only one service provider in each embodiment that provides the data to the user. There is no disclosure in Saito of providing a common public key to a plurality of service providers.

For the foregoing reasons, the references, even when combined, fail to teach or suggest each limitation of claim 1.

The above notwithstanding, claim 1 is allowable over the prior art of record for at least the additional reason that one of ordinary skill in the art would not find it obvious to modify Kudelski in view of Saito. Kudelski teaches:

> The code or key of permutation is transmitted in real time so that even if a pirate finds the right combination, this one is only valid for a very short instant of time, e.g. one second.

(col. 4, lines 50-53). Thus, Kudelski does not suffer from a problem of unauthorized access to programming. One of ordinary skill in the art would not seek to modify Kudelski by importing teachings of Saito to encrypt the access information with a shared public key.

As noted above, part of the invention of claim 1 is the recognition of the desirability of using a single smart card to access content from several different

service providers. Thus, there is no suggestion or teaching in the prior art to modify the references as proposed by the Examiner.

For at least the foregoing reasons, claim 1 is allowable over the prior art of record.

Claims 2-4 and 15-17 depend ultimately from claim 1, and are allowable at least by reason of their dependence from allowable base claim 1.

Rejection of claims 6 and 11 under 35 USC 103(a) as being unpatentable over Kudelski (US Pat No 5144663) in view of Saito, and further in view of EBU Project Group, "Functional Model of a Conditional Access System"

The EBU Project Group reference is cited as teaching a smart card used in a conditional access system that uses the PCMCIA standard.

Applicants submit that the alleged teachings of the EBU Project Group reference still fail to cure the defect of Kudelski and Saito as applied to claim 1, and as such, claim 6 is patentably distinguishable over the suggested combination of references.

Ser. No. 09/743,653
Internal Docket No. RCA 89131
CUSTOMER NO. 24498

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

Ahmet Mursit Eskicioglu et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: November 10, 2006